FIG. 1

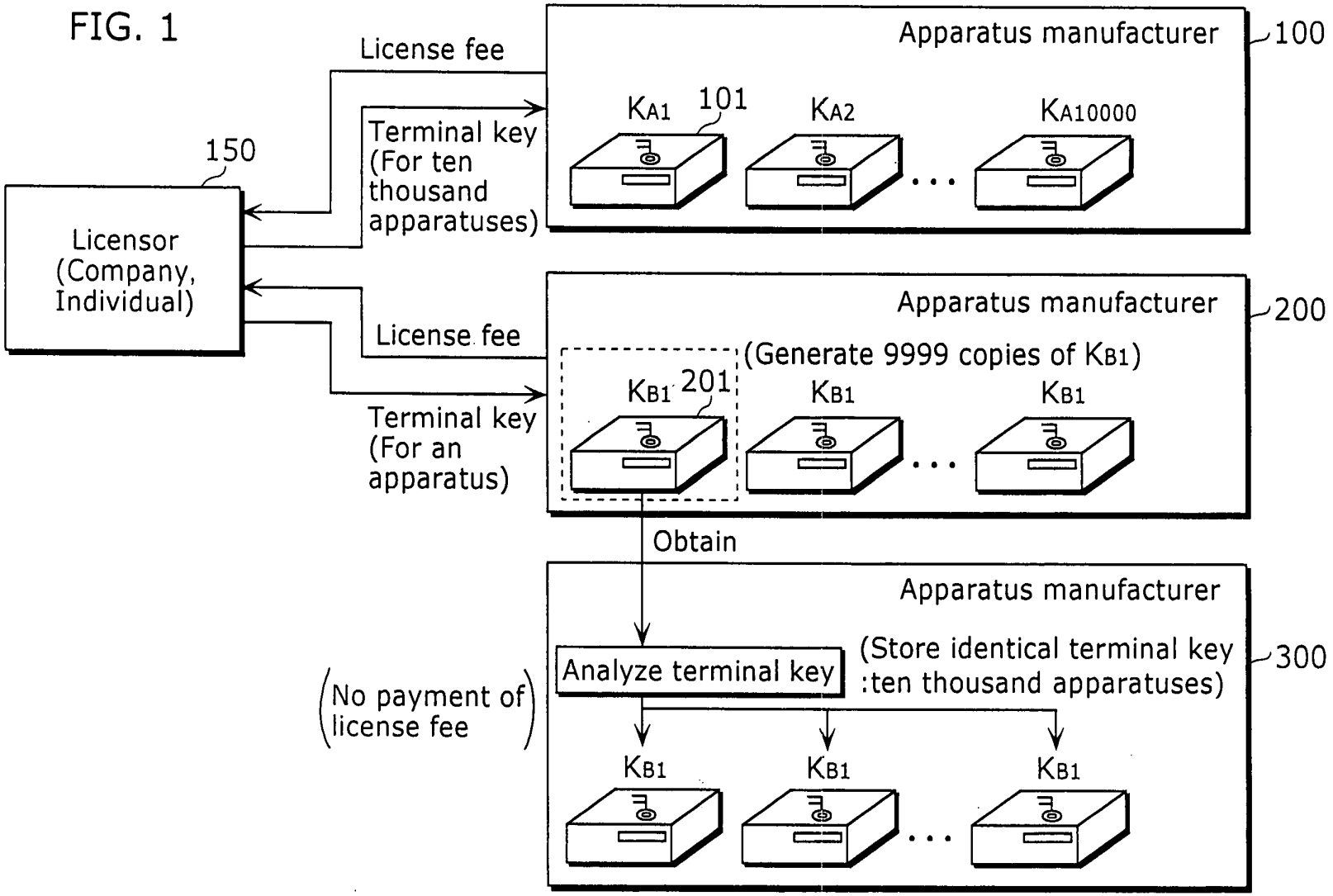

Apparatus manufacturer
100
101
K_{A1}
K_{A2}
K_{A10000}
License fee
Terminal key
(For ten
thousand
apparatuses)
150
Licensor
(Company,
Individual)
Apparatus manufacturer
200
(Generate 9999 copies of K_{B1})
201
K_{B1}
License fee
Terminal key
(For an
apparatus)
Obtain
Apparatus manufacturer
300
Analyze terminal key
(Store identical terminal key
:ten thousand apparatuses)
No payment of
license fee

FIG. 2

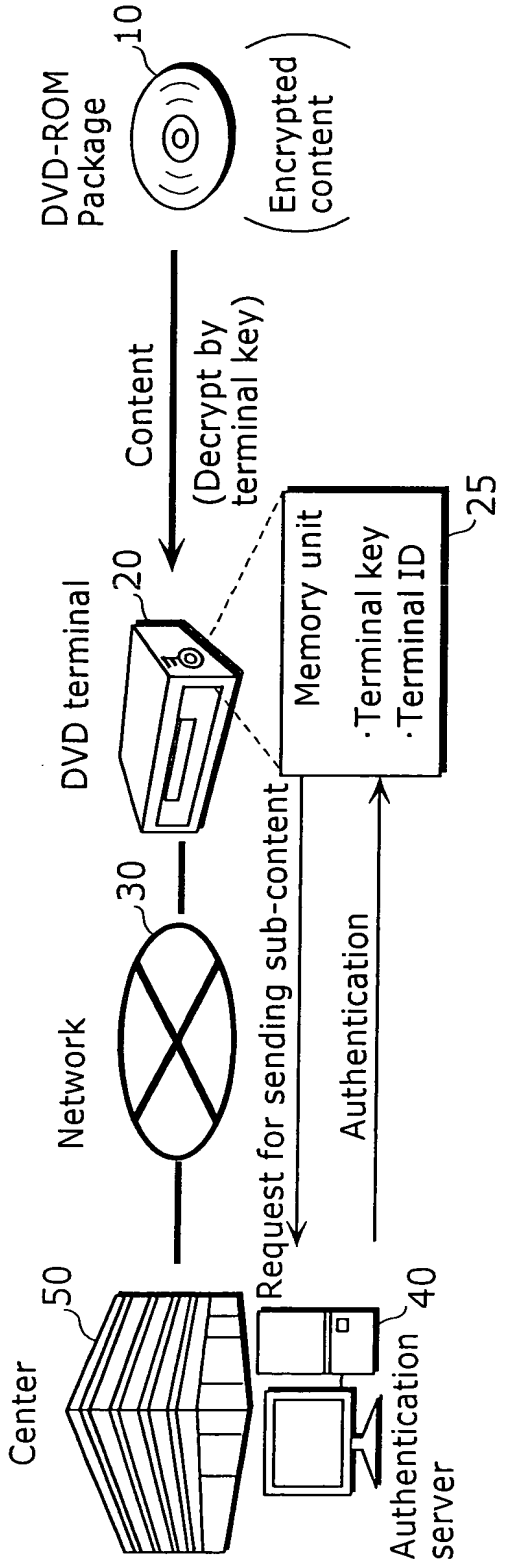

5
DVD-ROM Package
10
Encrypted content
Content
(Decrypt by terminal key)
DVD terminal
20
Memory unit
·Terminal key
·Terminal ID
25
Network
30
Request for sending sub-content
Authentication
Center
50
Authentication server
40

FIG. 3

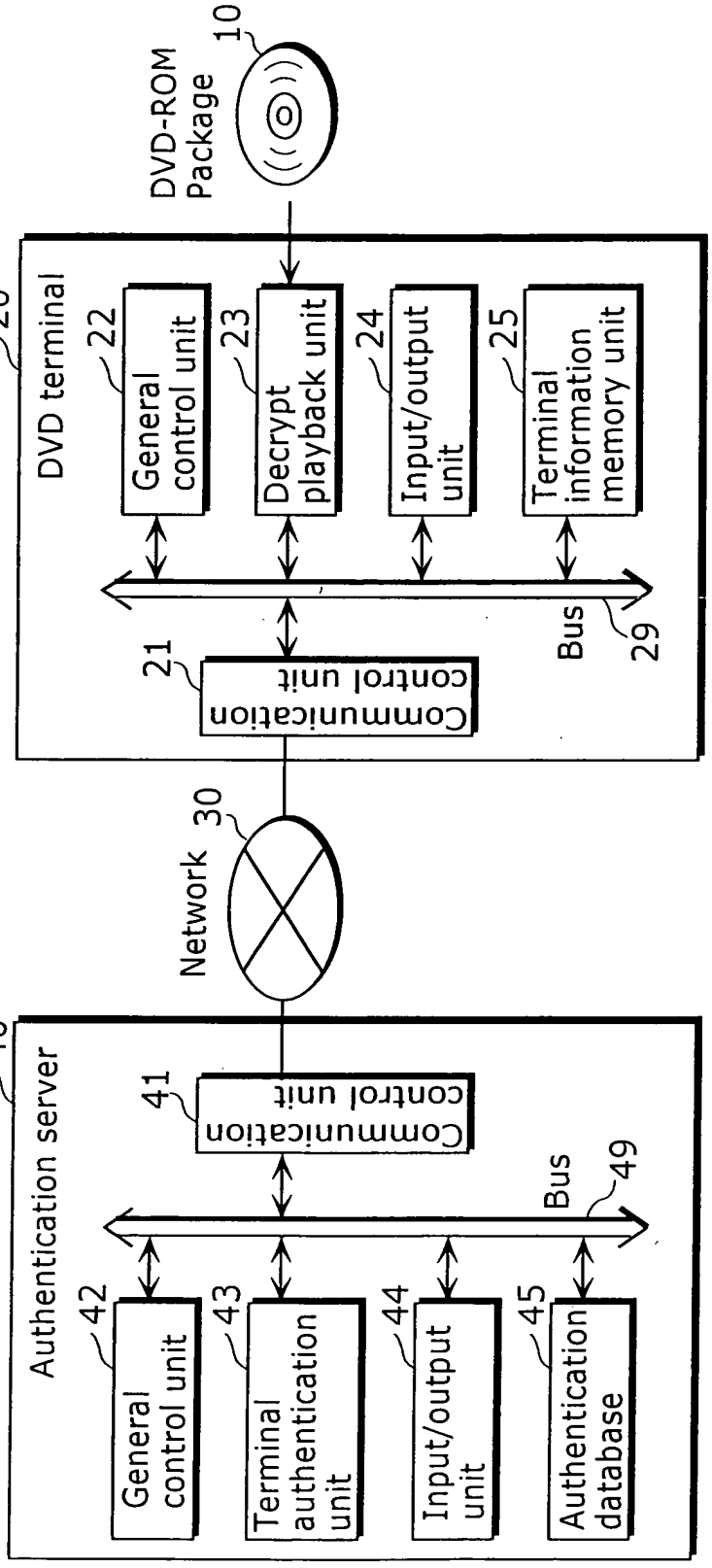

DVD-ROM Package
10
DVD terminal
20
General control unit
22
Decrypt playback unit
23
Input/output unit
24
Terminal information memory unit
25
Bus
29
Communication control unit
21
Network
30
Authentication server
40
Communication control unit
41
Bus
49
General control unit
42
Terminal authentication unit
43
Input/output unit
44
Authentication database
45

FIG. 4A

Model name+serial numbers	Terminal ID	Terminal key	Download history of sub-content
DVM-1234-NNNNN	ABC5566	DEF7890	Director's cut version ○○○
DVM-2345-NNNNN	UVW6677	XYZ8901	Making film △△△
⋮	⋮	⋮	⋮

FIG. 4B

Model name	Manufacturer name	Terminal key	Total number of terminal keys	Access number
DVM-1234	Company A	DEF 7890	10,000	18,500
DVM-5678	Company B	XYZ 8901	50,000	36,200
⋮	⋮	⋮	⋮	⋮

FIG. 5

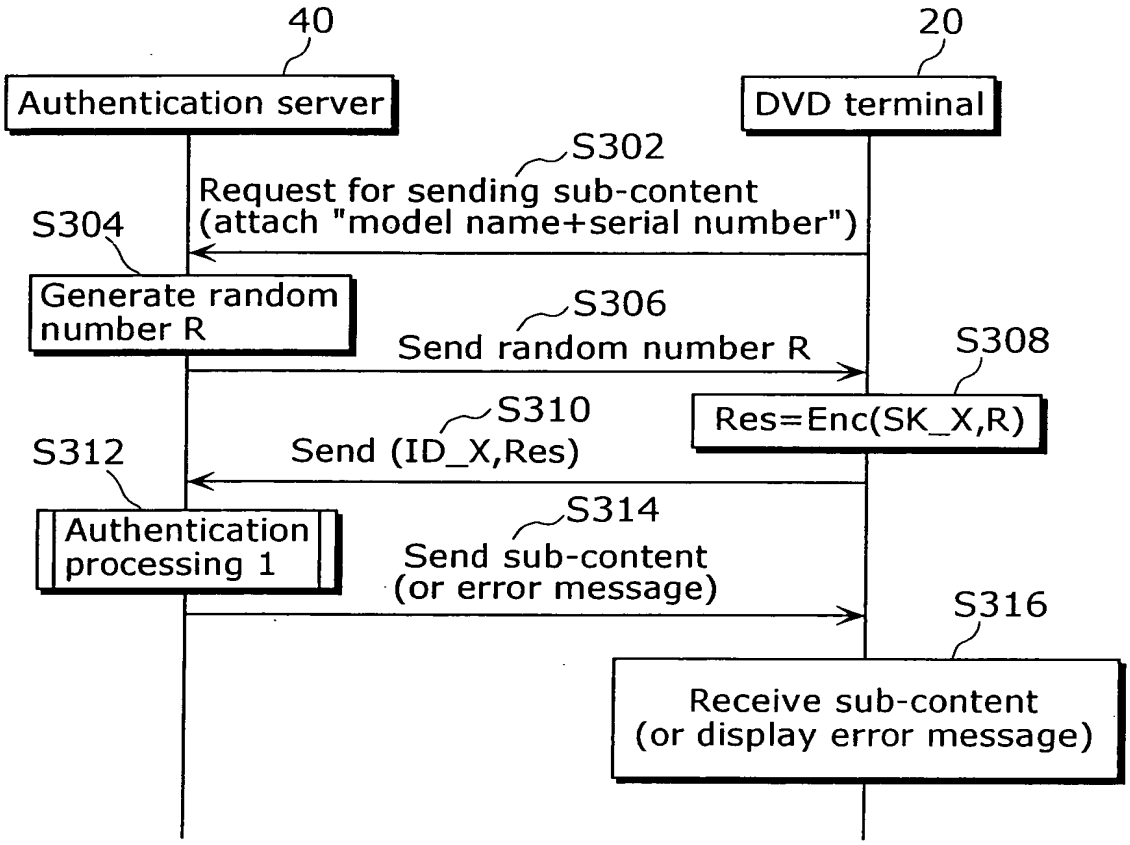

40
Authentication server
20
DVD terminal
S302
Request for sending sub-content
(attach "model name+serial number")
S304
Generate random number R
S306
Send random number R
S308
Res=Enc(SK_X,R)
S310
Send (ID_X,Res)
S312
Authentication processing 1
S314
Send sub-content
(or error message)
S316
Receive sub-content
(or display error message)

FIG. 6

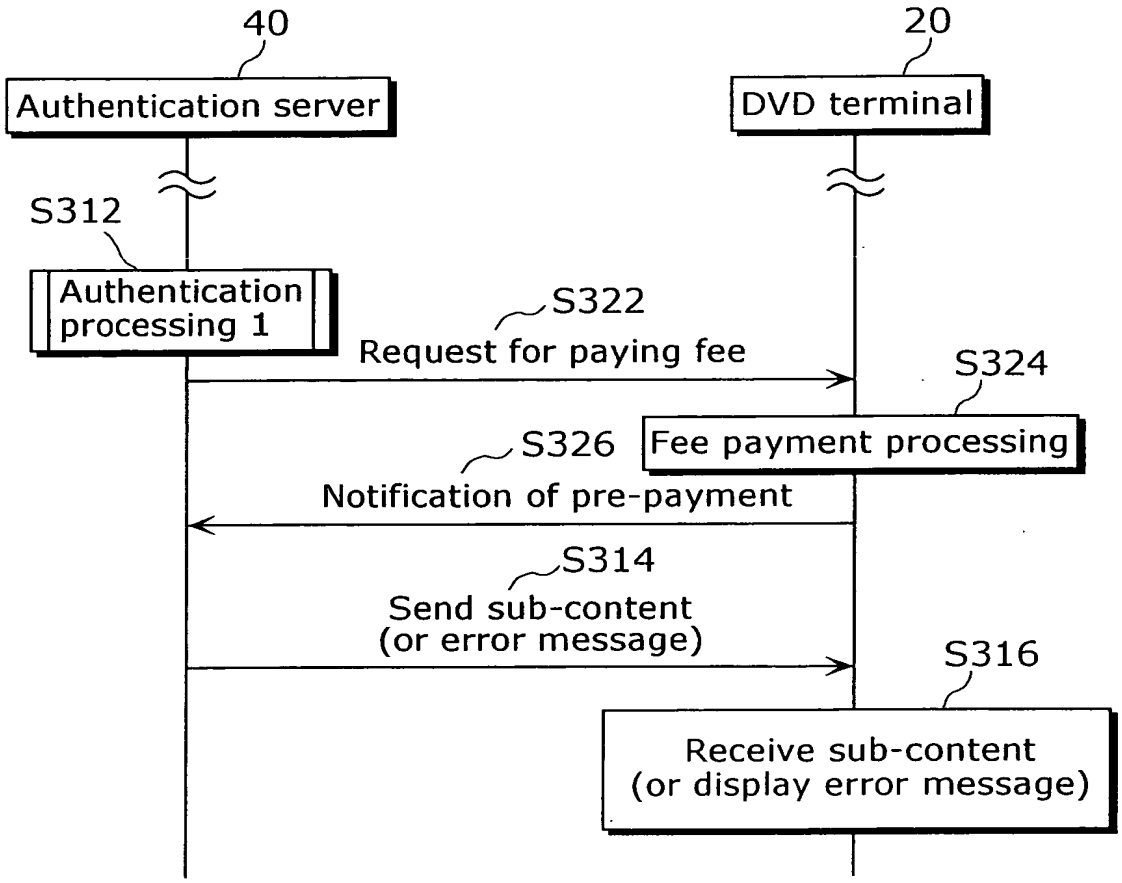

40
Authentication server
20
DVD terminal
S312
Authentication processing 1
S322
Request for paying fee
S324
Fee payment processing
S326
Notification of pre-payment
S314
Send sub-content (or error message)
S316
Receive sub-content (or display error message)

FIG. 7

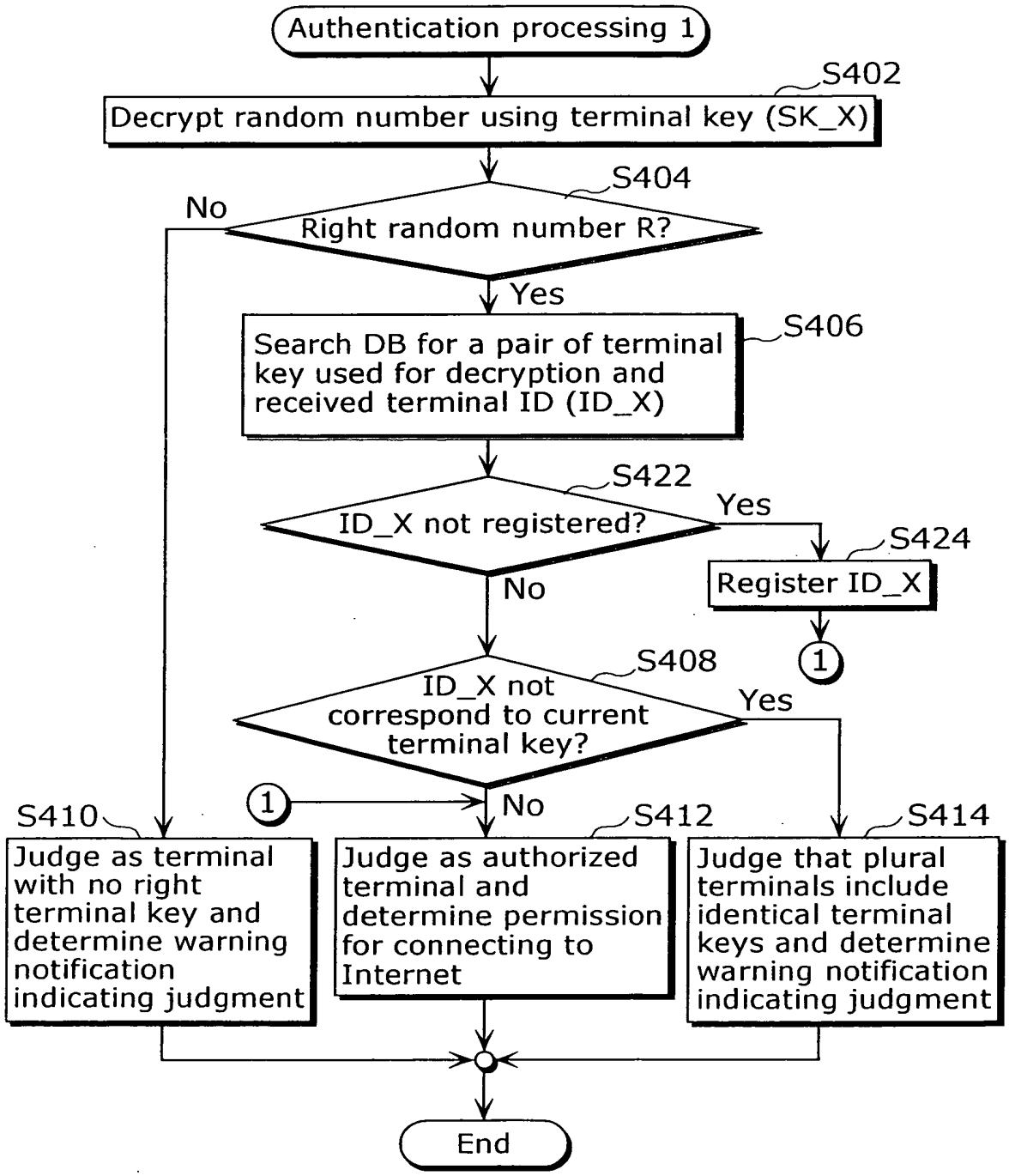

Authentication processing 1
S402
Decrypt random number using terminal key (SK_X)
S404
No
Right random number R?
Yes
S406
Search DB for a pair of terminal key used for decryption and received terminal ID (ID_X)
S422
ID_X not registered?
Yes
S424
Register ID_X
No
1
S408
ID_X not correspond to current terminal key?
Yes
1
No
S410
Judge as terminal with no right terminal key and determine warning notification indicating judgment
S412
Judge as authorized terminal and determine permission for connecting to Internet
S414
Judge that plural terminals include identical terminal keys and determine warning notification indicating judgment
End

FIG. 8

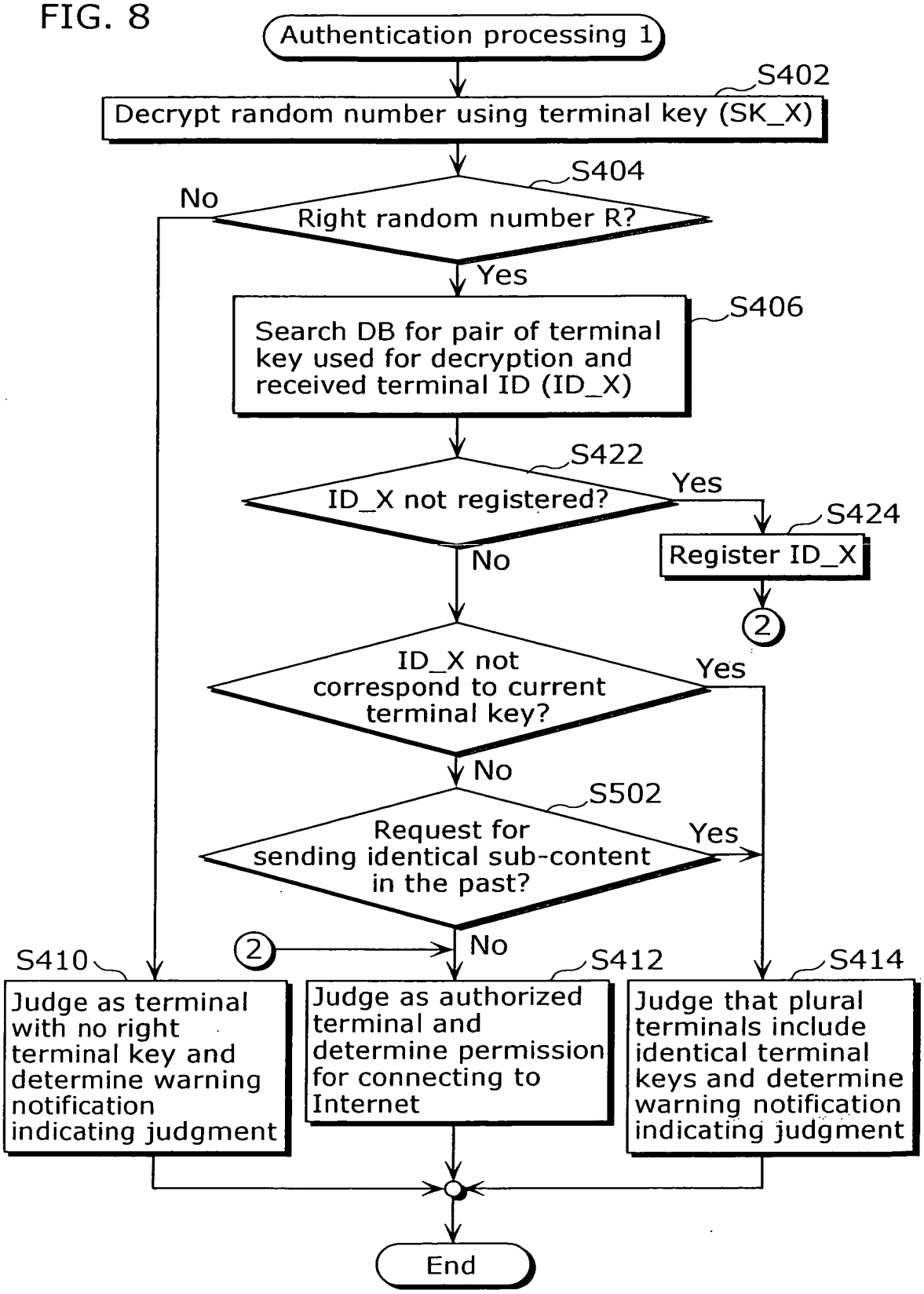

Authentication processing 1
S402
Decrypt random number using terminal key (SK_X)
S404
No
Right random number R?
Yes
S406
Search DB for pair of terminal key used for decryption and received terminal ID (ID_X)
S422
ID_X not registered?
Yes
S424
Register ID_X
2
No
ID_X not correspond to current terminal key?
Yes
No
S502
Request for sending identical sub-content in the past?
Yes
2
No
S410
S412
S414
Judge as terminal with no right terminal key and determine warning notification indicating judgment
Judge as authorized terminal and determine permission for connecting to Internet
Judge that plural terminals include identical terminal keys and determine warning notification indicating judgment
End

FIG. 9

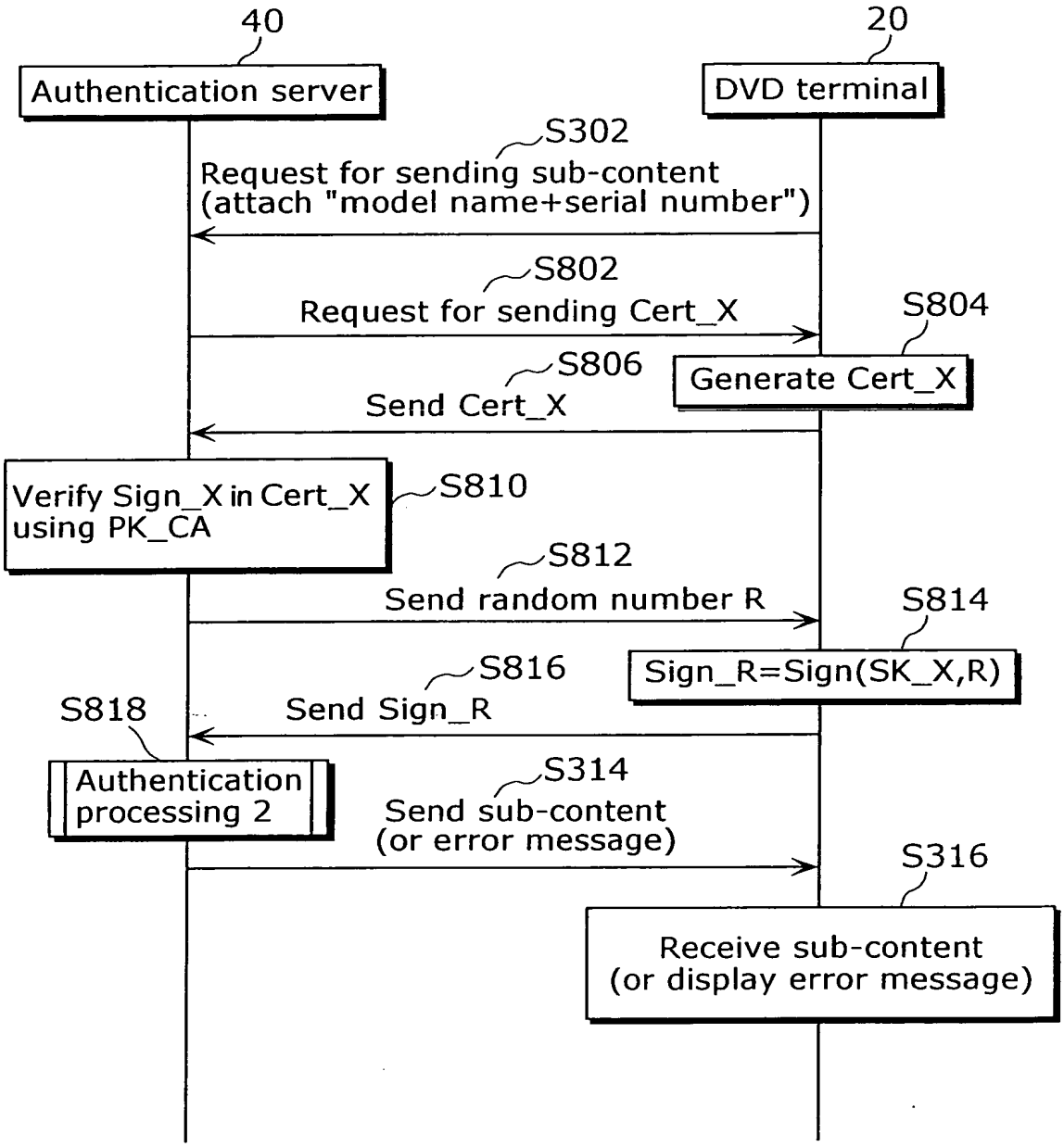
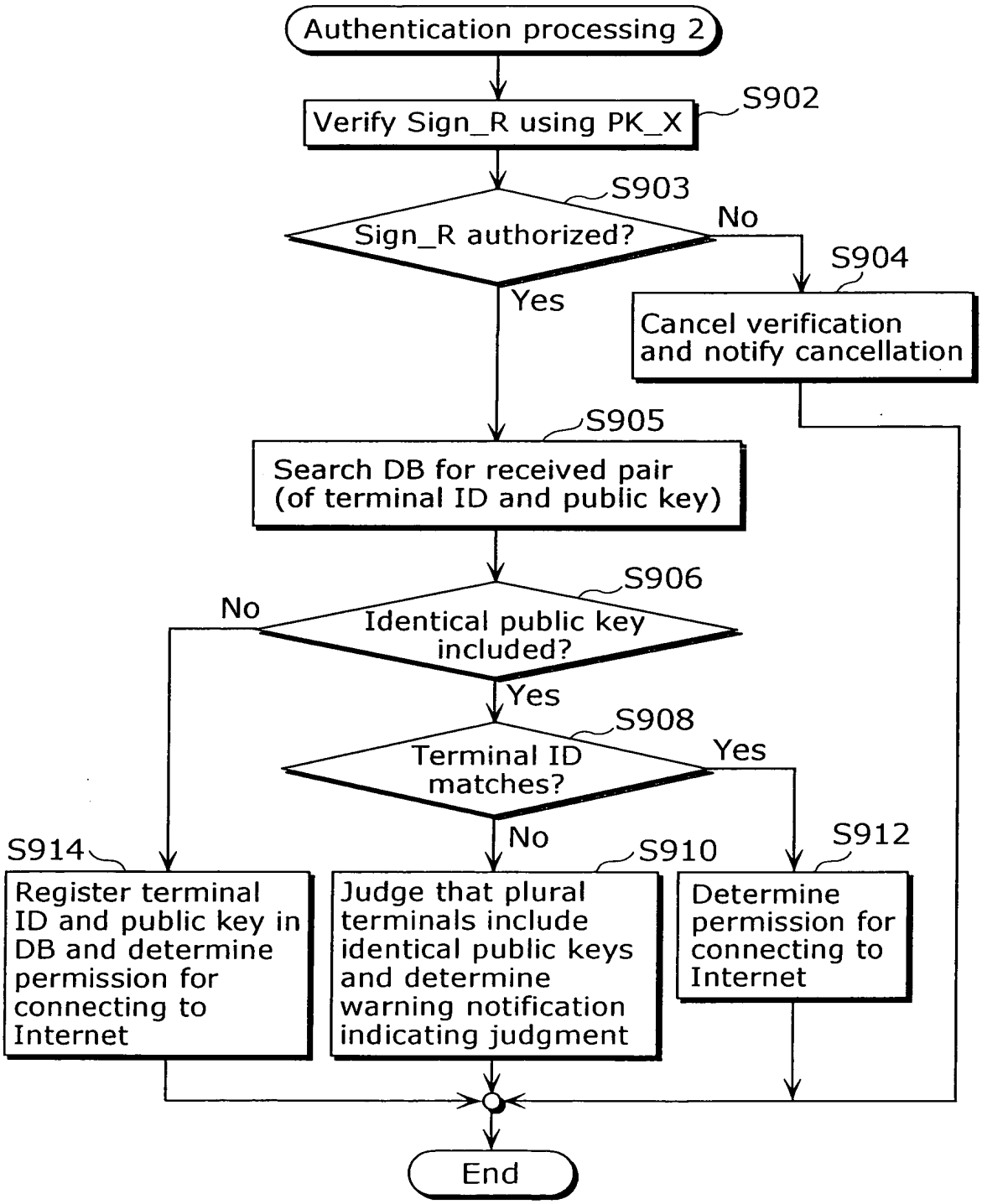

40
Authentication server
20
DVD terminal
S302
Request for sending sub-content
(attach "model name+serial number")
S802
Request for sending Cert_X
S804
Generate Cert_X
S806
Send Cert_X
Verify Sign_X in Cert_X
using PK_CA
S810
S812
Send random number R
S814
Sign_R=Sign(SK_X,R)
S816
Send Sign_R
S818
Authentication
processing 2
S314
Send sub-content
(or error message)
S316
Receive sub-content
(or display error message)

FIG. 10


Authentication processing 2
Verify Sign_R using PK_X
S902
S903
Sign_R authorized?
No
S904
Yes
Cancel verification and notify cancellation
S905
Search DB for received pair (of terminal ID and public key)
S906
No
Identical public key included?
Yes
S908
Terminal ID matches?
Yes
No
S914
S910
S912
Register terminal ID and public key in DB and determine permission for connecting to Internet
Judge that plural terminals include identical public keys and determine warning notification indicating judgment
Determine permission for connecting to Internet
End